Security and Privacy of Radio Frequency Identification

Rieback, M.R.

2008

document version
Publisher's PDF, also known as Version of record

SAMENVATTING

Beveiliging en Privacy van Radio Frequentie Identificatie

Radio Frequency Identification (RFID) tags zijn computerchips die op een afstand van energie (stroom) voorzien worden door hun uitleesapparaten. RFID tags worden beschouwd als de opvolger van de barcode. Ze bieden bieden draadloze identificatie, en beloven een revolutie in industriële, commerciële en medische toepassingen. RFID tags bieden een gemakkelijke manier om informatie over fysieke objecten te verzamelen. Het voordeel van RFID tags is dat zij informatie over meerdere objecten kunnen bevatten en dat zij van een afstand en door fysieke barrières uitgelezen kunnen worden. Binnen de "ubiquitous computing" visie van Mark Weiser kunnen RFID tags onze interacties met computinginfrastructuur uitgroeien tot iets onbewusts en fantastisch.

RFID chips zijn in het algemeen net zo groot als een korreltje rijst, en zij hebben ingebouwde logica en een analoog frontend. Passieve (en semi-actieve) RFID tags worden volledig gevoed door middel van energie die ze krijgen van hun RFID lezers, en daarentegen gebruiken actieve tags batterijen waardoor zij een groter bereik hebben. Low frequency (LF) tags (125–135 kHz) zijn uitleesbaar tot 30 centimeter, high frequency (HF) tags (13.56 MHz) tot 1 meter, ultra high frequency (UHF) tags (860–960 MHz en 2.45 GHz) tot 7 meter, en actieve tags tot 100 meter of meer.

RFID tags worden gepresenteerd als een technologie om kosten te besparen door efficiëntie van het zaken doen te verhogen, om transparantie in de logistiek te verbeteren, en om pervasive of embedded computing te implementeren. Met RFID tags vervagen dus de grenzen tussen de online-wereld en de fysieke wereld. Daardoor maakt RFID een tal van nieuwe toepassingen mogelijk binnen toegangsbeheer, automatisering van de detailhandel, (slimme) huizen en kantoren, en het opsporen van mens en dier.

PROBLEEMSTELLING

Ondanks de talloze voordelen, heeft RFID ook een duistere kant. Dezelfde gebruikersvriendelijkheid en beschikbaarheid die RFID zo revolutionair maakt geeft minder ethische mensen ongekende mogelijkheden tot diefstal, geheime opsporing en gedragsprofilering. Zonder afdoende toegangsbeheer kunnen aanvallers ongehinderd RFID tags lezen, en daardoor de locatie van mensen of objecten bespioneren, RFID tags klonen, data van RFID tags wijzigen, of de communicatie tussen RFID tags and RFID lezers verstoren.

Er is een manier nodig om RFID tags (zelfs de allergoedkoopste) in de gaten te houden en tegen misbruik te beschermen. Om de privacy te beschermen is het nodig om op een gebruikersvriendelijke manier om de RFID beveiligingsfunctionaliteit te coordineren, door nauwkeurige uitvoering van audits, sleutelmanagement, toegangsbeheer, en authenticatie via de RFID interface.

RFID installaties moeten aan de hand van beveiligingsaudits en penetratietesten beoordeeld worden net zoals andere computersystemen. Organisaties die RFID systemen ingebruik nemen hebben de verantwoordelijkheid om de beveiliging van hun installaties op de proef te stellen, maar zij weten vaak niet hoe ze dit moeten doen. Dit is iets wat de computerbeveiligingsindustrie wel op wil pakken, maar veel beveiligingsexperts hebben een gebrek aan de geschikte testapparatuur voor RFID systemen. Het is dus van belang dat dergelijke testapparatuur ontwikkeld wordt en beschikbaar komt voor beveiligingsexperts (en ontwikkelaars op het gebied van RFID).

BIJDRAGEN

In dit proefschrift introduceer ik het concept “RFID malware” en beschrijf ik het ontwerp, implementatie, en evaluatie van de “RFID Guardian”, het eerste geïntegreerde platform voor RFID beveiliging en privacybeheer.

RFID Malware

In dit proefschrift beschrijf ik het concept van RFID malware, in het bijzonder RFID exploits, RFID wormen en RFID virussen. RFID systemen hebben een aantal aspecten die ze kwetsbaar en aantrekkelijk voor aanvallers maken: veel en complexe broncode, het gebruik van standaardprotocollen en technologieën, het gebruik van databasen en het aanwezigheid van waardevolle data.

RFID exploits zijn enkelgebruik aanvallen waarbij kwaadaardige data op RFID tags gebruikt wordt om achterliggende software componenten aan te vallen. RFID exploits misbruiken dus specifieke systeemcomponenten zoals databases, webin-

terfaces, en gluecode door middel van bekende aanvallen zoals buffer-overflows, code-insertion, en SQL-injectie. Kort samengevat, lanceren RFID exploits standaard "hack aanvallen", zoals overal te vinden op het Internet zijn, door goedkope, passieve RFID tags en contactloze kaarten, of door apparaten die RFID tags emuleren.

Een RFID worm is zichzelf voortplantende code dat netwerkverbindingen gebruikt om zichzelf te propageren naar databasen en nieuwe RFID tags . Wormen hebben vaak een zogenaamde "payload", die verwoestingen aanricht zoals het wissen van bestanden, informatie stiekem versturen via email of het installeren van "backdoors".

Een RFID virus is code die zichzelf kan voortplanten zonder de aanwezigheid van een netwerkverbinding; RFID tags zijn voldoende om RFID virusaanvallen te verspreiden. RFID virussen gebruiken RFID exploits om achterliggende RFID systemen te modificeren op een zodanige manier dat de data van nieuwe RFID tags worden voorzien van de code van het RFID virus. Zelfreferentieële commando's en quines zijn twee manieren om de volledige aanvalscode naar de juiste databaselocatie te schrijven. Ook RFID virussen kunnen voorzien worden van een schadelijke payload.

Systeembeheerders en ontwikkelaars van RFID middleware kunnen aanvallen op RFID systemen afweren door gebruik te maken van de volgende technieken: bounds-checking, het opschonen van invoer, het uitzetten van script-interpretors, het beperken van permissies, het scheiden van gebruikers, het binden van parameters, isolatie van de middleware server, en het voldoende reviewen van RFID middleware broncode.

RFID Guardian

De RFID Guardian is een mobiel, batterij-gevoed apparaat dat "bemiddeld" in interacties tussen RFID lezers en RFID tags .

Te bescherming van de privacy biedt de RFID Guardian een "RFID firewall". De huidige RFID countermeasures implementeren vaak hun beveiligingspolicies op de RFID tags; dit maakt de policies echter moeilijk te configureren en te gebruiken. Om deze situatie te verbeteren, wij hebben een RFID lezer met RFID tag emulatie gecombineerd in een platform dat de onderlinge coordinatie van RFID countermeasures mogelijk maakt. Individuele beveiligingspolicies worden dan afgedwongen door de unieke functies van de RFID Guardian (auditing, automatisch sleutelbeheer, bemiddeling tussen RFID tags en RFID lezers, off-tag authentication) samen met bestaande RFID beveiligingstechnieken (kill-commando's, slaap/waak modes, on-tag cryptografie). Andere doelstellingen van de RFID Guardian zijn: gedrag dat afhankelijk is van de context, gebruikersvriendelijkheid, en toepasbaarheid in de "echte wereld".

De RFID Guardian is ontworpen als een soort van “zwitsers zakmes” voor RFID beveiliging, met daarin een geïntegreerd pakket van beveiligingstesten: diagnostiek en monitoren, manipulatie en filteren van RFID pakketten, penetratietesten en side-channel aanvallen. Zo’n toolkit is essentieel voor het fatsoenlijk testen van de aanvalsbestendigheid van RFID systemen, waardoor eigenaren van RFID systemen goed onderbouwde afwegingen kunnen maken tussen beveiliging en gebruiksgemak voor een bepaalde toepassing.

We hebben de RFID Guardian gebouwd met behulp van standaardcomponenten, en onze ervaringen bevestigen dat actieve, mobiele apparaten zijn nuttig voor het beveiligen van RFID tags in verschillende toepassingen, inclusief de bescherming van goedkope tags die zichzelf anders niet kunnen beschermen.